The $\exists^*\forall^*$ Part of the Theory of Ground Term Algebra Modulo an AC Symbol is Undecidable[1]

Jerzy Marcinkowski[2]

Institute of Computer Science, University of Wrocław, ul. Przesmyckiego 20, 51-165 Wrocław, Poland
E-mail: jma@ii.uni.wroc.pl

Received September 15, 1999; revised November 29, 2000; published online August 20, 2002

We show that the $\exists^*\forall^*$ part of the equational theory modulo an AC symbol is undecidable. This solves the open problem 25 from the RTA list. We show that this result holds also for the equational theory modulo an ACI symbol.

Key Words: unification; equational theories; decidability.

1. INTRODUCTION

Formulae built of terms and the equality predicate are one of the most natural objects in rewriting. One of the most natural ways of modeling the semantic behavior of real objects is considering additional equality axioms between terms. The most natural set of equality axioms is AC, that is the associativity axiom $f(x, f(y, z)) = f(f(x, y), z)$ and the commutativity axiom $f(x, y) = f(y, x)$. Validity of an equational formula modulo AC is in general an undecidable problem. This paper is not the first attempt to demarcate the decidability–undecidability border, that is to find the classes of the "simple" formulas, for which there exists an algorithm deciding validity.

We consider a finite signature $\mathcal{S}$ of function symbols, containing also some AC symbols. We also assume that there is at least one constant in the signature, so the set of ground terms over $\mathcal{S}$ is not empty. Then we consider the first order equational theory of the ground term algebra over $\mathcal{S}$: the only relational symbol of the theory is the equality, the function symbols are the symbols in $\mathcal{S}$, and the variables range over the set of ground terms.

The measure of the complexity of a formula is the number of alternations of quantifiers in the prenex form. On the undecidability side of the border it was proved in [10] and [11] that the Σ_3 part of the theory is undecidable (this part contains the formulae whose quantifier prefix is of the form $\exists^*\forall^*\exists^*$). On the decidability side, it is known that the Σ_1 part (existential formulas) is decidable [C93]. Also several papers (including [6] and [5]) were written about the decidability of some special cases of the so-called *AC complement problem*, which itself is a special case of the Σ_2 part of the theory. Decidability of the whole Σ_2 part was stated as an open problem in [10] and then on the RTA list of open problems [2–4, 9]. In this paper we present the negative solution to the problem.

The rest of the paper is organized as follows: in Section 2 we prove undecidability of the existential-universal (Σ_2) part of the theory of an AC idempotent symbol: we assume there is a function symbol in the signature which is not only commutative and associative but also idempotent, which means that it satisfies the axiom $f(x, x) = x$. In Section 3 we present our main result: undecidability of the $\exists^*\forall^*$ theory of an AC symbol. In Section 4 we prove the result of Section 3 for the smallest possible signature and in Section 5 we show that the main result holds also if infinite terms are allowed. Finally, in Section 6 we discuss some related questions.

2. $\exists^*\forall^*$ THEORY OF ONE IDEMPOTENT AC SYMBOL

Let us start from a very simple case of the equational theory of an idempotent AC symbol. In [10] and [11] Treinen shows that the $\exists^*\forall^*\exists^*$ part of the theory is undecidable. We begin this technical part

[1] This paper is the extended version of [7].
[2] Supported by Polish KBN Grant 8 T11C 043 19.

0890-5401/02 $35.00

showing the undecidability of the $\exists^*\forall^*$ part of the theory. It will be a good introduction to the methods used in the following sections.

Let $\Pi = \{\langle l_1, r_1\rangle, \langle l_2, r_2\rangle \dots \langle l_k, r_k\rangle\}$ be an instance of the Post correspondence problem. This means that each l_i and r_i is a nonempty word over some finite alphabet (we assume it is $\{a, b\}$). Let us recall that a nonempty word $w = j_1 j_2 \dots j_s$ over the alphabet $\{1, 2, \dots k\}$ is called *a solution of* Π if $l_{j_1} l_{j_2} \dots l_{j_s} = r_{j_1} r_{j_2} \dots r_{j_s}$ and that the existence of a solution is an undecidable property of Π.

We consider the signature consisting of the binary ACI symbol $+$, two unary function symbols a and b, and the function symbol h of arity 2. The only constant is c.

The words l_i, r_i can be naturally understood as unary contexts built over the signature $\{a, b\}$: for example the word abb means for us the same as the context $a(b(b(X)))$.

Let us define:

$$\begin{aligned}
\chi_1(x) = \forall w, w_1, w_2 \quad & \\
& (h(w_1, w_2) + w = x \wedge (w_1 \neq w_2 \vee w_1 = w_2 = c)) \Rightarrow \\
& [h(l_1(w_1), r_1(w_2)) + w + h(w_1, w_2) = x \vee \\
& h(l_2(w_1), r_2(w_2)) + w + h(w_1, w_2) = x \vee \\
& \dots \\
& \vee\, h(l_k(w_1), r_k(w_2)) + w + h(w_1, w_2) = x)] \\
\chi_2(x) = \exists s \;\; & h(c, c) + s = x
\end{aligned}$$

and

$$\chi = \exists x \;\; \chi_1(x) \wedge \chi_2(x).$$

Obviously χ is an $\exists^*\forall^*$ formula. It is convenient to think that h is a pair constructor here, c is the end of a string, and $+$ is the set union.

THEOREM 1.

1. *Formula χ is valid if and only if Π is solvable.*
2. *The $\exists^*\forall^*$ part of the equational theory modulo an idempotent AC symbol is undecidable.*

Of course (ii) follows from (i). The proof of (i) is left for the reader as an easy exercise. Let us, however, explain the meaning of the formulas above. The existentially quantified variable x is understood as a "set." Formula χ_2 says that the pair ε, ε of words, encoded as $h(c, c)$, is "in x." This happens to be the "first pair of the solution of the PCP instance Π" but what is important here is that this pair is the initialization of some process, whose termination is undecidable. Formula $\chi_1(x)$ says that if a pair $h(w_1, w_2)$ is in x then one of the possible next configurations of the process is also in x (unless $h(w_1, w_2)$ encodes the final configuration of the process). Since we consider first order terms, the set represented by x is finite. So it can only exist if the process terminates (a similar proof can be given also if we accept infinite terms, see Section 5 for details). The technical problem is how to say "is in x" by a universal formula. To express the fact that $y \in x$ we need a "witness" w, such that $w + y = x$. However, using such a witness may lead to a $\exists^*\forall^*\exists^*$ formula: *There exists such an x that the initial configuration is in x and for every configuration y and every witness w if $y + w = x$, which means if y is in x, then there exists a witness v such that $v + u_1 = x$ or $v + u_2 = x$ or $\dots v + u_k = x$, where $u_1, u_2, \dots u_k$ are possible configurations reachable from y in one step*. Let us note that the last is exactly the formula from Treinen's proof [10, 11].

In this section we could get rid of one quantifier alternation (that is, go from the $\exists^*\forall^*\exists^*$ formula to the $\exists^*\forall^*$ formula) without major changes in the original proof. This was the case since we were able to reuse the witness: thanks to the idempotency v can be built as $w + h(w_1, w_2)$. To our knowledge no simple trick of this kind would be sufficient for the proof of Theorem 2, where a nonidempotent AC symbol is considered.

3. $\exists^*\forall^*$ THEORY OF AN AC SYMBOL

In this section we prove our main result:

THEOREM 2. *The $\exists^*\forall^*$ equational theory modulo an AC symbol is undecidable.*

As explained in Section 2 if $+$ is not idempotent then a common sense attempt to write a formula *if $h(t_1, t_2)$ in x then also $h(t_1', t_2')$ in x* would make use of existentially quantified witness y, such that $y + h(t_1', t_2') = x$. But then we will end up with an $\exists\forall\exists$ formula rather than $\exists\forall$. In order to overcome this problem we will keep in x not only "configurations of a process" but also, together with each configuration, a witness of the membership of a subsequent configuration. This is why instead of the binary symbol h we have the arity 4 symbol f in the signature now.

Let us define:

$$\phi_1(t_l, t_r, s_l, s_r) = (s_l = l_1(t_l) \wedge s_r = r_1(t_r)) \vee (s_l = l_2(t_l) \wedge s_r = r_2(t_r)) \vee \cdots \vee (s_l = l_k(t_l) \wedge s_r = r_k(t_r)).$$

The role of this subformula is similar to the one which is by χ_1 played in Section 2. It asserts that the pair s_l, s_r is reachable in one step of the computation process from the pair t_l, t_r.

The formula $\phi_2(x)$ will be first defined informally:

$$\begin{aligned}\phi_2(x) \;=\; & \forall w, z \;\; w + z = x \wedge w \text{ is of the form } f(w_1, w_2, w_3, w_4)\\ & \Rightarrow w \text{ is of the form } f(t_l, t_r, t,\, f(r_l, r_r, r, v)) \text{ or of the form } f(s, s, c, c) \text{ with } s \neq c.\end{aligned}$$

It may seem that we need a $\forall^*\exists^*$ prefix to write $\phi_2(x)$. This would lead to the $\exists^*\forall^*\exists^*$ formula ϕ below, and we would fail to prove Theorem 2. However, to our surprise, $\phi_2(x)$ can be written as a universal formula:

$$\begin{aligned}&\forall w, w_1, w_2, w_3, w_4, w_5\\ &\quad \neg(x = w + f(w_1, w_2, w_3, a(w_4)))\wedge\\ &\quad \neg(x = w + f(w_1, w_2, w_3, b(w_4)))\wedge\\ &\quad \neg(x = w + f(w_1, w_2, w_3, w_4 + w_5))\wedge\\ &\quad \neg[x = w + f(w_1, w_2, w_3, c) \wedge (w_3 \neq c \vee w_1 \neq w_2 \vee w_1 = c)].\end{aligned}$$

Notice that our proof will not work if the signature under consideration was infinite. This is because in such a case we would not be able to enumerate all the forbidden patterns, like we do above. In fact I do not know if the $\exists^*\forall^*$ part of the equational theory modulo AC is also undecidable for an infinite signature (which may sound strange, since an infinite signature seems to be a more complicated object than a finite one, and intuitively should lead to "more undecidable" theories).

Define:

$$\begin{aligned}\phi_3(x) = \forall y, s_l, s_r, t, r_l, r_r, w, v\\ f(s_l, s_r, t,\, f(r_l, r_r, w, v)) + y = x \Rightarrow\\ \phi_1(s_l, s_r, r_l, r_r) \wedge w + f(r_l, r_r, w, v) = t.\end{aligned}$$

The formula $\phi_3(x)$ is the engine of our recursion vehicle. In the proof of Lemma 2 you are going to see it working. The last subformula we need to define is $\phi_4(x)$, which is the starter of our engine:

$$\phi_4(x) = \exists s_1, s_2 \quad x = s_1 + f(c, c, s_1, s_2).$$

Now, define ϕ as

$$\exists x \;\; \phi_2(x) \wedge \phi_3(x) \wedge \phi_4(x).$$

ϕ is clearly an $\exists^*\forall^*$ formula.

LEMMA 1. *If Π is solvable then ϕ is valid.*

Proof. If Π is solvable then there exists a finite sequence $x_0, y_0, x_1, y_1 \ldots x_l, y_l$ of terms such that $x_0 = y_0 = c$ and $\phi_1(x_i, y_i, x_{i+1}, y_{i+1})$ holds for each $i = 0, 1, \ldots l-1$ and that $x_l = y_l$.

Define $t_l = f(x_l, y_l, c, c)$. When t_j is defined for some $j > 0$ as $f(s_1, s_2, s_3, s_4)$ define t_{j-1} as

$$f(x_{j-1}, y_{j-1}, s_3 + f(s_1, s_2, s_3, s_4), f(s_1, s_2, s_3, s_4)).$$

Then define $x = t_0 + t_1 + \cdots + t_l + c$.

Notice that if t_j is $f(s_1, s_2, s_3, s_4)$ for some $j \geq 0$ then $s_1 = x_j$ and $s_2 = y_j$. If $x = w + f(s_1, s_2, s_3, s_4)$ for some s_1, s_2, s_3, s_4 then $f(s_1, s_2, s_3, s_4)$ is t_j for some j and so we can check directly that ϕ_2 and ϕ_3 hold for x.

To prove that ϕ_4 also holds first notice that $t_0 = f(c, c, s_3, s_4)$ for some s_3 and s_4. Then use induction to show that if t_j is $f(r_1, r_2, r_3, r_4)$ then $r_3 = c + t_l + \cdots + t_{j+1}$. So $s_3 = c + t_l + \cdots + t_1$ and $x = t_0 + s_3$. ■

LEMMA 2. *If ϕ is valid then Π is solvable.*

Suppose ϕ is valid and let x be such a term that $\phi_2(x) \wedge \phi_3(x) \wedge \phi_4(x)$ holds.

Take such s_1 and s_2 that $x = s_1 + f(c, c, s_1, s_2)$. They exist since $\phi_4(x)$ holds. Define t_0 as $f(c, c, s_1, s_2)$. Now, if t_j is defined for some j and t_j is of the form $f(z_1, z_2, z_3, f(w_1, w_2, w_3, w_4))$ then define t_{j+1} as $f(w_1, w_2, w_3, w_4)$.

LEMMA 3. *For every $i \geq 0$, if t_i is defined as $f(z_1, z_2, z_3, z_4)$ then*

1. *Either $t_i + z_3 = x$ or there exists w such that $w + t_i + z_3 = x$.*
2. *$z_1 = z_2$ or t_{i+1} is defined.*
3. *Suppose t_{i+1} is defined as $f(u_1, u_2, u_3, u_4)$ for some terms u_1, u_2, u_3, u_4. Then $\phi_1(z_1, z_2, u_1, u_2)$ holds.*
4. *If t_{i+1} is defined as $f(u_1, u_2, u_3, u_4)$ for some terms u_1, u_2, u_3, u_4 then u_1 is larger than z_1 (has more symbols).*

Proof of Lemma 3. Notice that for given i claim (ii) follows from (i) (since $\phi_2(x)$ is valid). Claim (iii) follows from (i) and (ii) (since $\phi_3(x)$ is valid). Claim (iv) follows from (iii).

If i is 0 then claim (i) follows from ϕ_4.

Suppose that the lemma holds for some $i-1$ and that t_i is defined.

Let $t_{i-1} = f(z_1, z_2, z_3, f(w_1, w_2, w_3, w_4))$. By hypothesis either $t_{i-1} + z_3 = x$ or there exists w such that $w + t_{i-1} + z_3 = x$. Since $z_3 = f(w_1, w_2, w_3, w_4) + w_3$ we get that either $t_{i-1} + f(w_1, w_2, w_3, w_4) + w_3 = x$ or $w + t_{i-1} + f(w_1, w_2, w_3, w_4) + w_3 = x$.

Now, notice that by Lemma 3 (i) for every defined t_i there exists w such that $w + t_i = x$. But for given x there are only finitely many such terms v that there exists w such that $x = v + w$. On the other hand, if $i \neq j$ and t_i and t_j are defined then they are different (this is by Lemma 3 (iv)). That implies that there exists l such that $t_l = f(z_1, z_2, z_3, z_4)$ is defined but t_{l+1} is not. By Lemma 3 (ii) this implies that $z_1 = z_2$. Consider the sequence $r_1^0, r_2^0, \ldots r_1^l, r_2^l$ of the first and second arguments of $t_0, t_1, \ldots t_l$ respectively. By Lemma 3 (iii) $\phi_1(r_1^i, r_2^i, r_1^{i+1}, r_2^{i+1})$ holds for each $i < l$. Since $r_1^0 = r_2^0 = c$ and $r_1^l = r_2^l$ this sequence is a solution of Π. ■

Theorem 2 follows now from Lemma 1, Lemma 2, and the undecidability of the Post correspondence problem.

4. THE SIMPLEST POSSIBLE SIGNATURE

Now we are going to show that Theorem 2 holds also if we restrict the signature so that it contains only the binary AC symbol $+$, a unary function symbol g, and a constant c. This is the simplest case in which undecidability can be conjectured. As noticed in [10] without g (that is if we only have the

AC symbol and some number of constants in the signature) the theory is decidable for the same reasons as Presburger arithmetic is (one can proceed here as in [8]).

In the proof of Theorem 2 we decided to use the Post correspondence problem as the one to which we reduce our problem. This was mainly an aesthetic choice. A Turing machine, for example, could do the job as well. In this case f in formula ϕ_1 should be of arity 5: instead of the two Post words we would encode the state of the finite control, the tape to the left of the head, and the tape to the right of the head. Technically this choice would not change anything, just the notations would be a little bit more complicated. Another possible choice could be a machine with two counters.

The first trouble that we have in this section with the Post correspondence problem is that if we want to encode it like in formula ϕ_1 then we need two different monadic function symbols a and b: PCP for words over an alphabet containing only one symbol is decidable. To get around this obstacle we will encode words in $\{a, b\}^*$ as numbers:

DEFINITION 1. For a given word $w \in \{a, b\}^*$ let $\mathbf{c}(w)$ (or code of w) be the natural number (in decimal notation) obtained by replacing all the symbols a of w by 1 and all the symbols b of w by 2.

The following obvious lemma states the property of the encoding $\mathbf{c}$ which will be useful in our construction:

LEMMA 4. *If w, l are words over $\{a, b\}$ then $\mathbf{c}(wl) = \mathbf{c}(l) + 10^{|l|}\mathbf{c}(w)$, where $|l|$ is the length of l.*

Define $\psi_1^i(x, y, z, t)$ as the formula

$$z = x + x + \cdots + x + \mathbf{c}(l_i) \wedge t = y + y + \cdots y + \mathbf{c}(r_i),$$

where x is added $10^{|l_i|}$ times and y is added $10^{|r_i|}$ times.

Now we are ready to write the formula ψ_1, which is a counterpart of the formula ϕ_1 from the previous section:

$$\psi_1(x, y, z, t) = \psi_1^1(x, y, z, t) \vee \psi_1^2(x, y, z, t) \vee \cdots \vee \psi_1^l(x, y, z, t).$$

In order to write the formula ψ_2, the counterpart of ϕ_2 we need a trick to get rid of the arity 4 function symbol. We can use $+$ instead; thanks to the associativity it has any arity we need. The problem is that, due to commutativity, we forget the order of the arguments then. Informally,

$$\begin{aligned}\psi_2(x) \;=\; &\forall w, z \;\; w + z = x \wedge w \text{ is of the form } g(u)\\ &\Rightarrow u \text{ is of the form } gggg(u_1) + ggg(u_2) + gg(u_3) + g(u_4),\end{aligned}$$

where none of u_1, u_2, u_3, u_4 has g at the root and either u_4 is of the form $gggg(v_1) + ggg(v_2) + gg(v_3) + g(v_4)$ where none of v_1, v_2, v_3, v_4 starts with g or $u_4 = u_3 = c$ and $u_1 = u_2 \neq c$.

Like ϕ_2, ψ_2 can also be written as a universal formula, but one must really be patient here:

$\forall w, z, u_1, u_2, u_3, u_4, u_5, v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8$

(1) $\neg(g(c + u_1) + z = x)\wedge$

(2) $\neg(g(g(u_1)) + z = x)\wedge$

(3) $\neg(g(g(u_1) + g(u_2)) + z = x)\wedge$

(4) $\neg(g(g(u_1) + g(u_2) + g(u_3)) + z = x)\wedge$

(5) $\neg(g(u_1 + u_2 + u_3 + u_4 + u_5) + z = x)\wedge$

(6) $\neg(g(ggggg(u_1) + u_2) + z = x)\wedge$

(7) $\neg(g(gggg(u_1) + gggg(u_2) + u_3) + z = x)\wedge$

(8) $\neg(g(ggg(u_1) + ggg(u_2) + ggg(u_3) + u_4) + z = x)\wedge$

(9) $\neg(g(gg(u_1) + gg(u_2) + gg(u_3) + gg(u_4) + z = x)\wedge$

(10) $\neg[[g(g(u_1) + g(u_2) + u_3) + z = x] \wedge [u_1 = v_1 + v_2 \vee u_1 = c] \wedge [u_2 = v_3 + v_4 \vee u_2 = c]]\wedge$

$$
\begin{aligned}
&(11)\ \neg[[g(gg(u_1)+gg(u_2)+u_3)+z=x]\wedge\\
&\quad [u_1=v_1+v_2\vee u_1=c]\wedge[u_2=v_3+v_4\vee u_2=c]]\wedge\\
&(12)\ \neg[[g(ggg(u_1)+ggg(u_2)+u_3)+z=x]\wedge\\
&\quad [u_1=v_1+v_2\vee u_1=c]\wedge[u_2=v_3+v_4\vee u_2=c]]\wedge\\
&(13)\ \neg[g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(c))+z=x\wedge(u_1\neq u_2\vee u_3\neq c)]\wedge\\
&(14)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(c+v_1)+z=x))\wedge\\
&(15)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(g(v_1))+z=x))\wedge\\
&(16)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(g(v_1)+g(v_2))+z=x))\wedge\\
&(17)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(g(v_1)+g(v_2)+g(v_3)))+z=x)\wedge\\
&(18)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+\\
&\qquad +gggg(g(v_1)+g(v_2)+g(v_3)+g(v_4)+g(v_5)))+z=x)\wedge\\
&(19)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(ggggg(v_1)+v_2))+z=x)\wedge\\
&(20)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(gggg(v_1)+gggg(v_2)+v_3))+z=x)\wedge\\
&(21)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(ggg(v_1)+ggg(v_2)+ggg(v_3)+v_4))+z=x)\wedge\\
&(22)\ \neg(g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(gg(v_1)+gg(v_2)+gg(v_3)+gg(v_4)))+z=x)\wedge\\
&(23)\ \neg[[g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(g(v_1)+g(v_2)+v_3))+z=x]\wedge\\
&\quad [v_1=v_5+v_6\vee v_1=c]\wedge[v_2=v_7+v_8\vee v_2=c]]\wedge\\
&(24)\ \neg[[g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(gg(v_1)+gg(v_2)+v_3))+z=x]\wedge\\
&\quad [v_1=v_5+v_6\vee v_1=c]\wedge[v_2=v_7+v_8\vee v_2=c]]\wedge\\
&(25)\ \neg[[g(g(u_1)+gg(u_2)+ggg(u_3)+gggg(ggg(v_1)+ggg(v_2)+v_3))+z=x]\wedge\\
&\quad [v_1=v_5+v_6\vee v_1=c]\wedge[v_2=v_7+v_8\vee v_2=c]].
\end{aligned}
$$

The first line of the formula says that if $g(u)+z=x$ then u does not have c as a summand. The lines from (2) to (4) say that such u is a sum of at least four summands. The fifth line says that u is not a sum of five summands or more. So here we already know that there are exactly four summands in such u and all of them have g at the root. The sixth line says that no summand in u is of the form $ggggg(v)$. At this point we know that u is a sum of four summands, each of them of one of the forms $g(v)$, $gg(v)$, $ggg(v)$, or $gggg(v)$, where v does not start with g. Since the formula is universal we cannot say now *for each of the four forms there is a summand in u which has this form*. Instead we say, in lines (7)–(12), *There is at most one summand of each of those forms*. To be more precise, in line (7) we say *There is at most one summand of the form gggg(v), where v is any term*. In line (8) we say *there are at most two summands of the form ggg(v), where v is any term* (we know that one of them has also the form $gggg(v)$) and in line (9) we say *there are at most three summands of the form gg(v), where v is any term*. But still we must exclude the possibility that there is more than one summand of each of the forms $g(v)$, $gg(v)$, and $ggg(v)$. This is done in the lines (10)–(12).

At this point only u_4 from the informal definition of ψ_2 needs to be described. Line (13) says that if u_4 is c then u_3 is also c and u_1 and u_2 are equal. In the lines (14)–(19) we repeat the trick from lines (1)–(6) to ensure that u_4 is a sum of four summands, each of them of the form $g(v)$, $gg(v)$, $ggg(v)$, or $gggg(v)$, where v does not start from g. Then, in the lines (20)–(22) we repeat the trick from lines (7)–(9) to ensure that u_4 is of the form $g(v_1)+gg(v_2)+ggg(v_3)+gggg(v_4)$, where none of the $v_1,\dots v_4$ begins with g. Finally, in the lines (23)–(25) we repeat, for u_4, the trick from lines (10)–(12).

Now we are ready to write ψ_3, the counterpart of ϕ_3,

$$
\begin{aligned}
\psi_3(x) \;=\;& \forall\, w, v, w_1, w_2, w_3, v_1, v_2, v_3, v_4\\
x \;=\;& w+g(g(w_1)+gg(w_2)+ggg(w_3)+gggg(g(v_1)+gg(v_2)+ggg(v_3)+gggg(v_4)))\\
\Rightarrow\;& \psi_1(w_1,w_2,v_1,v_2)\wedge w_3=v_3+g(g(v_1)+gg(v_2)+ggg(v_3)+gggg(v_4))
\end{aligned}
$$

and ψ_4, the counterpart of ϕ_4:

$$\psi_4(x)=\exists s_1,s_2\quad x=s_1+g(g(\mathbf{c}(l_1)+gg(\mathbf{c}(r_1)+ggg(s_1)+gggg(s_2)))).$$

Notice that we could not postulate the existence "in x" of a term with the codes $\mathbf{c}(\varepsilon)$ in the two first positions (as it was done in ϕ_4). This is because $\mathbf{c}(\varepsilon)$ is zero, and we only know how to count positive natural numbers. That is why we use a slightly different version of the Post correspondence problem. The following lemma is an obvious consequence of the undecidability of the standard version of the Post correspondence problem:

LEMMA 5. *The existence of a solution $l_{i_1} l_{i_2} \dots l_{i_m} = r_{i_1} r_{i_2} \dots r_{i_m}$ of an instance Π of the post correspondence problem remains undecidable even if we require that $i_1 = 1$.*

Finally, we write formula ψ. It is not very hard to guess that ψ is:

$$\exists x \ \psi_2(x) \wedge \psi_3(x) \wedge \psi_4(x).$$

Clearly, ψ is a $\exists^*\forall^*$ formula.

Now the undecidability of the $\exists^*\forall^*$ part of the theory over the signature with only a single monadic function symbol and one constant follows from:

LEMMA 6. *ψ is valid if and only if Π solvable.*

To prove the lemma one can simply repeat the proofs of Lemmas 1 and 2, with the obvious notational changes.

5. INFINITE TERMS

In this section we assume that the quantification ranges over (possibly) infinite terms. It turns out that, with only some minor modifications, we can also repeat for this case the result and method of Section 3.

Let us start from the remark that one can imagine two different definitions of what equality modulo an AC symbols means. The first possibility is that we consider two infinite terms equal only if their equality can be proved in a finite number of AC-steps. The second possibility is that we allow an infinite number of AC-steps. The proof below works for both cases.

The main difference between the situation in this section and the one in Section 3 is that we cannot write here: *There exists x such that the initial configuration is in x, and together with a nonterminal configuration y the set x contains one of the configurations reachable from y in one step*. If we allow infinite terms then x as required by the formula exists even if the process does not terminate. Instead the formula should be: *There exists x such that the initial configuration is in x, such that together with every configuration y the set x contains all the configurations reachable from y in one step and such that no terminal configuration is in x*.

To write this formula one can for example consider the signature with the function symbol f of arity $k + 3$, where k is the number of pairs in the PCP.

The formula θ_1 will be:

$$\theta_1(w, v, w_1, v_1, w_2, v_2, \dots w_k, v_k) = w_1 = l_1(w) \wedge v_1 = r_1(v) \wedge w_2 = l_2(w) \wedge v_2 = r_2(v) \wedge \dots w_k = l_k(w) \wedge v_k = r_k(v).$$

We are going to give only an informal description of θ_2. The reader who understood Sections 3 and 4 can easily imagine how to write it formally as a universal formula.

$\theta_2(x) = \forall w, u$

$w + u = x \wedge w$ is of the form $f(y_l, y_r, y, y_1, y_2, \dots y_k) \Rightarrow$

($y_l \neq y_r$ or $y_l = y_r = c$) and each of $y_1, y_2, \dots y_k$ is of the form

$f(v_l, v_r, v, v_1, v_2, \dots v_k)$

$\theta_3(x) = \forall w, y_l, y_r, y, v_l^1, v_r^1, v^1, v_1^1, v_2^1, \dots v_k^1, v_l^2, v_r^2, v^2, v_1^2, v_2^2, \dots v_k^2 \dots v_l^k, v_r^k, v^k, v_1^k, v_2^k, \dots v_k^k$

$$
\begin{aligned}
x = w + f(y_l, y_r, y,\\
&f\big(v_l^1, v_r^1, v^1, v_1^1, v_2^1, \dots v_k^1\big),\\
&f\big(v_l^2, v_r^2, v^2, v_1^2, v_2^2, \dots v_k^2\big),\\
&\dots\\
&f\big(v_l^k, v_r^k, v^k, v_1^k, v_2^k, \dots v_k^k\big)) \Rightarrow\\
\big[y = f\big(v_l^1, v_r^1, v^1, v_1^1, v_2^1, \dots v_k^1\big) + v^1 +\\
&+ f\big(v_l^2, v_r^2, v^2, v_1^2, v_2^2, \dots v_k^2\big) + v^2 + \cdots\\
&\cdots + f\big(v_l^k, v_r^k, v^k, v_1^k, v_2^k, \dots v_k^k\big) + v^k \wedge\\
&\theta_1\big(y_l, y_r, v_l^1, v_r^1, v_l^2, v_r^2, \dots v_l^k, v_r^k\big)\big]\\
\theta_4(x) = \exists s, s_1, s_2, \dots s_k \quad x = s + f(c, c, s, s_1, s_2, \dots s_k)
\end{aligned}
$$

and

$$\theta = \exists x \quad \theta_2(x) \wedge \theta_3(x) \wedge \theta_4(x).$$

Now, θ is false if and only if Π is solvable.

6. DISCUSSION

6.1. Terms with Bounded AC-Depth

A careful reader might have noticed the principal difference between Treinen's undecidability proof for the $\forall^*\exists^*\forall^*$ part of the equational theory modulo an AC symbol and our proof for the $\exists^*\forall^*$ part of the equational theory modulo an AC idempotent symbol, as described in Section 2, on one side, and our proof for the $\exists^*\forall^*$ part of the equational theory modulo an AC symbol on the other side. Briefly speaking, the existentially quantified terms in Section 2 do not have much of the AC structure. To make things more precise we need the notion of AC-depth of a term. By AC-depth of a term we denote the maximal number of alternations between the AC symbol and ordinary function symbols on a path from the root of a term to one of its leaves:

DEFINITION 2.

1. The AC-depth of a constant is 0;

2. if f is an ordinary (i.e., non-AC) function symbol then the AC-depth of $f(t_1, t_2, \dots t_k)$ is the maximal AC-depth of the terms $t_1, t_2, \dots t_k$;

3. The AC-depth of $s + t$ is the maximal AC-depth of the terms s and t if they both have $+$ in the root;

4. The AC-depth of $s + t$ is 1 plus the maximal AC-depth of the terms s and t if they both have ordinary function symbols in the root;

5. if s has $+$ in the root and t has an ordinary function symbol in the root then the AC-depth of $s + t$ is equal to the AC-depth of s if it is greater than the AC-depth of t and is equal to 1 plus the AC-depth of t otherwise.

An equivalent and maybe more convenient way is to to think about flattened terms: We agree that $+$ can have any arity ≥ 2, and apply to a given term t an (infinite) rewriting system whose rules are those of the form:

$$+(+(s_1, s_2, \dots s_n), r_1, r_2, \dots r_m) \Rightarrow +(s_1, s_2, \dots s_n, r_1, r_2, \dots r_m).$$

The unique normal form of t is called a flattened version of t (remember that $+$ is commutative). Now,

it is easy to see that the AC-depth of t, as defined above, is exactly the maximal number of $+$ symbols on a path from the root of the flattened version of t to one of its leaves.

For a given k let us call *k-bounded equational theory modulo an AC symbol* the equational theory where the quantifiers only range over terms of AC-depth bounded by k. Obviously the k-bounded theory is not a part (a subset) of the real equational theory modulo an AC symbol. It is very easy to construct a sentence which is valid in one of them but not in the other. For example the formula

$$\exists x, y, z, t \;\; y = f(x) + c \wedge z = f(y) + c \wedge t = f(z) + c$$

is valid in the equational theory modulo AC but not in the 3-bounded theory. But the techniques of Section 2 prove:

THEOREM 3. *Let $k \geq 2$. Then the $\forall^*\exists^*\forall^*$ part of the k-bounded equational theory modulo an AC symbol and the $\exists^*\forall^*$ part of the k-bounded equational theory modulo an AC idempotent symbol are undecidable even if the quantifiers only range over terms of AC-depth bounded by some fixed $k \geq 2$.*

The theorem above shows how little use we make in Section 2 of the AC symbol. Things are different in Section 3: the proof method there does not work for the bounded theory. It is easy to observe that the existential quantified term described by the $\exists^*\forall^*$ formula, if it really exists, needs to have AC-depth equal to the minimal number of pairs giving a solution of the instance of the post correspondence problem.

I would be very curious to know if an undecidability proof in the style of Section 2 is possible for the $\exists^*\forall^*$ theory. In other words I would find it interesting to know if the $\exists^*\forall^*$ fragments of the bounded theories are decidable (it may of course happen that the answer depends on the bound k).

6.2. AC Complement Problem

The most interesting restricted fragment of the $\exists^*\forall^*$ part of the theory of the ground term algebra modulo an AC symbol is known as *the AC complement problem*. The question here is to decide, for given terms (with variables) $t_1, t_2, \ldots t_k$, if the complement of the set of their ground instances is nonempty. The last holds if and only if the $\exists^*\forall^*$ formula

$$\exists t \;\forall s_1, s_2, \ldots s_l \; t \neq t_1 \wedge t \neq t_2 \wedge \cdots \wedge t \neq t_k$$

is valid, where $s_1, s_2, \ldots s_l$ are all the variables from $t_1, t_2, \ldots t_k$.

In [6] and [5] proofs of decidability of some very special cases of the AC complement problem can be found. For example [6] shows that the problem is decidable if all the terms t_i are linear. There are also reports about work in progress on this subject [9]. But despite this effort decidability of the AC complement problem remains open. In particular, we do not see how we could modify the method that we give in Section 3 to get an undecidability result here: the instances of AC complement problem only allow negative information concerning equalities in the existentially quantified term, while we need, at least as far as I see, a lot of positive information there, for example in ϕ_3.

ACKNOWLEDGMENT

Many thanks to ToMasz Wierzbicki for the discussion which opened my eyes. I also thank the anonymous referees who found many typos and small bugs in the submitted version.

REFERENCES

1. Comon, H. (1993), Complete axiomatizations of some quotient term algebras, *Theoret. Comput. Sci.* **118**(2), 167–191.
2. Dershowitz, N., Jouannaud, J.-P., and Klop, J. W. (1991), Problems in rewriting, *in* "Proceedings of 4 RTA," Lecture Notes in Computer Science, Vol. 448, pp. 445–456, Springer-Verlag, Berlin.
3. Dershowitz, N., Jouannaud, J.-P., and Klop, J. W. (1993), More problems in rewriting, *in* "Proceedings of 5th RTA," Lecture Notes in Computer Science, Vol. 690, pp. 468–487, Springer-Verlag, Berlin.
4. Dershowitz, N., Jouannaud, J.-P., and Klop, J. W. (1995), Problems in rewriting III, *in* "Proceedings of RTA 95," Lecture Notes in Computer Science, Vol. 914, pp. 457–471, Springer-Verlag, Berlin.

5. Fernandez, M. (1993), AC-Complement problems: Validity and negation elimination, *in* "Proceedings of 5th RTA," Lecture Notes in Computer Science, Vol. 690, pp. 358–373, Springer-Verlag, Berlin.
6. Lugiez, D., and Moysset, J.-L. (1993), Complement problems and tree automata in AC-like theories, *in* "Proceedings of the Symposium on Theoretical Aspects of Computer Science," Lecture Notes in Computer Science, Vol. 665, pp. 515–524, Springer-Verlag, Berlin.
7. Marcinkowski, J. (1999), Undecidability of the $\exists^*\forall^*$ part of the theory of ground term algebra modulo an AC symbol "Proceedings of RTA 99," Lecture Notes in Computer Science, Vol. 1631, pp. 92–102, Springer-Verlag, Berlin.
8. Machtey, M., and Young, P. (1978), "An Introduction to the General Theory of Algorithms," Elsevier, Amsterdam.
9. The RTA list of open problems maintained by Nachum Dershowitz and Ralf Treinen, *available at* http://www.lri.fr/~rtaloop/introduction.html.
10. Treinen, R. (1990), A new method for undecidability proofs of first order theories, *in* "Proceedings of the Tenth Conference on Foundations of Software Technology and Theoretical Computer Science," Lecture Notes in Computer Science, Vol. 472, Springer-Verlag, Berlin.
11. Treinen, R. (1992), A new method for undecidability proofs of first order theories, *J. Symbolic Comput.* **14**(5), 437–458.